ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ

**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»**

КАЛМЫЦКИЙ ФИЛИАЛ

УТВЕРЖДАЮ
Директор филиала
_____Э.Л. Пашнанов
«_1_» ___06___ 2022г.

# РАБОЧАЯ ПРОГРАММА
# УЧЕБНОЙ ПРАКТИКИ

по профессиональному модулю

02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

квалификация – техник по защите информации

Элиста, 2022 г.

УП 02
10.02.05

ОДОБРЕНА
Предметно-цикловой комиссией
естественнонаучных и
математических дисциплин
Протокол № 10
от «19» 04 2022 г.

Председатель ПЦК
Катрикова Ц.Ю. _____

Разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных

начальник учебно-методического отдела
Н.С. Бамбушева / _____

Составитель: _____ Пипенко В.В., высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»

Рецензенты: _____ Катрикова Ц.Ю., высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»

_____ Агеев С.С., ведущий администратор базы данных КУ РК «Центр учета и отчетности в организациях государственного сектора»

**РЕЦЕНЗИЯ**

на рабочую программу по учебной практике по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУ ИВО МГГЭУ Пипенко В.В.

Представленная рабочая программа учебной практики по профессиональному модулю ПМ. 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе современного Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре, примерных программ учебных дисциплин среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО, утвержденных Департаментом государственной политики и нормативно-1 правового регулирования в сфере образования Министерства образования и науки Российской Федерации.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения учебной практики (по профилю специальности), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций.

Учебная практика профессионального модуля направлена на получение первоначального практического опыта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

В тематическом плане и содержании учебной практике раскрываются виды и объем работ, выполняемых студентом во время практики, указывается распределение часов по учебным занятиям, необходимым для овладения конкретной профессиональной деятельностью, предусмотренной рабочей программой профессионального модуля по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в соответствии с ФГОС СПО.

Условия реализации учебной практики определяют требования к минимальному материально-техническому обеспечению, оборудованию учебного кабинета и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения учебной практики содержит результаты обучения и методы оценки.

Таким образом, рабочая программа учебной практики рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет».

Рецензент С.С. Агеев, ведущий администратор базы данных КУ РК «Центр учета и отчетности в организациях государственного сектора»

**РЕЦЕНЗИЯ**

на рабочую программу по учебной практике по профессиональному модулю ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами для специальности СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем, разработанную преподавателем Калмыцкого филиала ФГБОУ ИВО МГГЭУ Пипенко В.В.

Представленная рабочая программа разработана на основе современного Федерального государственного образовательного стандарта по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Структура рабочей программы соответствует структуре, примерных программ учебных дисциплин среднего профессионального образования на основе Федеральных государственных образовательных стандартов СПО, утвержденных Департаментом государственной политики и нормативно-1 правового регулирования в сфере образования Министерства образования и науки Российской Федерации.

В общей характеристике рабочей программы сформулированы цели и планируемые результаты освоения учебной практики (по профилю специальности), виды работ, обеспечивающих формирование профессиональных компетенций, количество часов, коды формируемых компетенций.

Учебная практика профессионального модуля направлена на получение первоначального практического опыта по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

В тематическом плане и содержании учебной практике раскрываются виды и объем работ, выполняемых студентом во время практики, указывается распределение часов по учебным занятиям, необходимым для овладения конкретной профессиональной деятельностью, предусмотренной рабочей программой профессионального модуля по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем в соответствии с ФГОС СПО.

Условия реализации учебной практики определяют требования к минимальному материально-техническому обеспечению, оборудованию учебного кабинета и техническим средствам обучения.

Информационное обеспечение обучения содержит современный перечень основных печатных источников, дополнительных печатных источников и электронных источников.

Контроль и оценка результатов освоения учебной практики содержит результаты обучения и методы оценки.

Таким образом, рабочая программа учебной практики рекомендуется к применению в учебном процессе Калмыцкого филиала ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет».

Рецензент  Катрикова Ц.Ю. высшая квалификационная категория, преподаватель Калмыцкого филиала ФГБОУ ИВО «Московский государственный гуманитарно-экономический университет»

СОДЕРЖАНИЕ

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1.В результате изучения профессионального модуля студент должен освоить вид деятельности Защита информации в автоматизированных системах программными и программно-аппаратными средствами и соответствующие ему профессиональные компетенции:

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ВД 2 | Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| ПК 2.1. | Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. |
| ПК 2.2. | Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. |
| ПК 2.3. | Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации. |
| ПК 2.4. | Осуществлять обработку, хранение и передачу информации ограниченного доступа. |
| ПК 2.5. | Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств. |
| ПК 2.6. | Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. |

1.1.2. Общие компетенции

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языках. |

| | |
|---|---|
| ОК 11. | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере. |

1.1.3. В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| Иметь практический опыт | – установки, настройки программных средств защиты информации в автоматизированной системе;<br>– обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами;<br>– тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации;<br>– решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации;<br>– применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных;<br>– учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности;<br>– работы с подсистемами регистрации событий;<br>– выявления событий и инцидентов безопасности в автоматизированной системе. |
| уметь | – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;<br>– диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;<br>– применять программные и программно-аппаратные средства для защиты информации в базах данных;<br>– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;<br>– применять математический аппарат для выполнения криптографических преобразований;<br>– использовать типовые программные криптографические средства, в том числе электронную подпись;<br>– применять средства гарантированного уничтожения информации;<br>– устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;<br>– осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак |
| знать | – особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; |

| | |
|---|---|
| | − методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации;<br>− типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;<br>− основные понятия криптографии и типовых криптографических методов и средств защиты информации;<br>− особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации;<br>− типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа. |

1.2. Воспитательная цель

В результате освоения учебной дисциплины в соответствии с рабочей программой воспитания образовательной программы среднего профессионального образования подготовки специалистов среднего звена по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем реализуется воспитательная цель - личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций специалистов среднего звена на практике.

Личностное развитие обучающихся и их социализация, проявляющиеся в развитии их позитивных отношений к общественным ценностям, приобретении опыта поведения и применения сформированных общих компетенций представлено следующими личностными результатами:

| **Личностные результаты реализации программы воспитания** *(дескрипторы)* | **Код личностных результатов реализации программы воспитания** |
|---|---|
| Осознающий себя гражданином и защитником великой страны | **ЛР 1** |
| Проявляющий активную гражданскую позицию, демонстрирующий приверженность принципам честности, порядочности, открытости, экономически активный и участвующий в студенческом и территориальном самоуправлении, в том числе на условиях добровольчества, продуктивно взаимодействующий и участвующий в деятельности общественных организаций | **ЛР 2** |
| **Личностные результаты реализации программы воспитания, определенные отраслевыми требованиями к деловым качествам личности** | |
| Демонстрирующий готовность и способность вести с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения в профессиональной деятельности | **ЛР 13** |
| Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности | **ЛР 14** |
| Проявляющий гражданское отношение к профессиональной | **ЛР 15** |

| | |
|---|---|
| деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем | |
| **Личностные результаты реализации программы воспитания, определенные субъектом Российской Федерации** (при наличии) | |
| Владеющий физической выносливостью в соответствии с требованиями профессиональных компетенций | **ЛР 17** |
| **Личностные результаты реализации программы воспитания, определенные ключевыми работодателями** (при наличии) | |
| Стрессоустойчивость, коммуникабельность | **ЛР 24** |

1.3. Рекомендуемое количество часов на освоение рабочей программы учебной практики по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами.

Рабочая программа рассчитана на прохождение обучающимися учебной практики для получения первичных профессиональных умений и навыков согласно учебного плана – 3 недели (108 часов).

## 2. СТРУКТУРА И СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

### 2.1. Тематический план учебной практики по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

| Виды и объем работ, выполненных студентом во время практики, согласно программе учебной практики | Кол-во часов |
|---|---|
| Настройка и оптимизация операционной системы; защита информации; настройка групповой политики; параметры входа в систему; настройка антивирусной программы; параметры сканирования; настройка серверной части антивирусной программы. | 21 |
| Разработка баз данных, форм, запросов и отчетов; создание прав пользователей. | 21 |
| Защита информации с помощью ПАК «Аккорд»; настройка учетных записей пользователей; администрирование системы; разграничение прав доступа; выявление ошибок и неисправностей ПАК «Аккорд»; выявление угроз безопасности ПАК; профилактика и обслуживание ПАК. | 22 |
| Решение задач, основ математической теории информации помехоустойчивого кодирования; применение простейших криптографических шифров для кодирования информации; вычисление электронной подписи; проверка электронной подписи; реализация криптографических методов. | 22 |
| Исследование безопасности ресурсов сети: средства идентификации и аутентификации; нахождение методов разделения ресурсов и технологии разграничения доступа; исследование средств создания резервных копии и восстановления баз данных, а также журнализации; исследование средств администратора безопасности баз данных и выполнение задач по обеспечению безопасности. | 22 |
| Итого | 108 |

2.2. Содержание учебной практики по профессиональному модулю 02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

| ПК/ОК | Содержание | Объем часов |
|---|---|---|
| ОК 1-11 ПК 2.1-2.6 | Настройка и оптимизация операционной системы. Защита информации. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Разработка политики безопасности. Установка атрибутов. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Настройка групповой политики. Параметры входа в систему. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Защита системных файлов. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Настройка антивирусной программы. Параметры сканирования. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Настройка серверной части антивирусной программы. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Разработка баз данных, форм, запросов и отчетов; | 4 |
| ОК 1-11 ПК 2.1-2.6 | Создание прав пользователей. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Защита БД. Пользователи БД и группы пользователей. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Защита информации с помощью ПАК «Аккорд». | 4 |
| ОК 1-11 ПК 2.1-2.6 | Настройка учетных записей пользователей. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Администрирование системы. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Разграничение прав доступа. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Выявление ошибок и неисправностей ПАК «Аккорд». | 4 |
| ОК 1-11 ПК 2.1-2.6 | Выявление угроз безопасности ПАК. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Профилактика и обслуживание ПАК. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Решение задач, основ математической теории информации помехоустойчивого кодирования. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Применение простейших криптографических шифров для кодирования информации. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Вычисление электронной подписи. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Проверка электронной подписи. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Реализация криптографических методов. | 4 |
| ОК 1-11 ПК 2.1-2.6 | Исследование безопасности ресурсов сети: средства идентификации и аутентификации. | 6 |
| ОК 1-11 ПК 2.1-2.6 | Нахождение методов разделения ресурсов и технологии разграничения доступа | 6 |
| ОК 1-11 ПК 2.1-2.6 | Исследование средств создания резервных копии и восстановления баз данных, а также журнализации. | 6 |
| ОК 1-11 ПК 2.1-2.6 | Исследование средств администратора безопасности баз данных и выполнение задач по обеспечению безопасности. | 6 |
| Промежуточная аттестация | | - |
| Итого | | 108 |

## 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

### 3.1. Требования к минимальному материально-техническому обеспечению

Для проведения учебной практики необходимо:

– помещения, в которых осуществляется практика, должны соответствовать действующим санитарным и противопожарным нормам, а также требованиям техники безопасности при проведении учебных и научно-производственных работ;

– предоставление рабочего места, оснащенного компьютером и иным оборудованием.

### 3.2. Информационное обеспечение обучения

3.2.1. Основные печатные источники:


1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2018. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8.


3.2.2. Дополнительные печатные источники:


1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие/ А.В.Васильков, И.А.Васильков.- М.: ФОРУМ,2010.- 368с.- (Профессиональное образование)
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/431080 (дата обращения: 16.12.2019).
3. Введение в криптографию/под.ред.В.В.Ященко/СПб.:Питер,2001.-288с.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
6. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
7. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
8. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

9. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
10. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
11. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
12. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
13. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
14. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
16. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
17. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.
18. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
19. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.
20. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
21. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
22. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин.

Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
23. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г.
№ 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
24. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
25. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
26. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
27. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
28. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
29. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
30. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
31. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
32. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
33. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
34. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
35. Сборник временных методик оценки защищенности конфиденциальной

информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
36. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
37. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
38. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкоссией России, 20ми02.
39. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
40. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
41. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.
    а) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;
    б) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.
42. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. - М.: Академия, 2016.
43. Голицына О.Л., Максимов Н.В., Попов И.И. «Базы данных» - Форум-Инфра-М, 2019 г.
44. Нечаев В. И. Элементы криптографии. Основы теории защиты информации. - М.: Высшая школа, 2019.
45. 15. В.Г. Жельников Криптография от папируса до компьютера. - М.: ABF, 2016.
46. Гринберг А.С. Защита информационных ресурсов государственного управления: учебное пособие для ВУЗов - М: ЮНИТИ-Дата, 2018.
47. Галатенко В.А. Стандарты информационной безопасности - М: ИНТУИТ.РУ, 2019.
48. Кулагин В.М. Международная безопасность: учебное пособие - М: Аспект-Пресс,2016.
49. Гришина Н.В. Организация комплексной защиты информации - М: Гелиос АРВ, 207

3.2.3. Электронные источники:

1. http://wm-help.net/books-online/book/98618/98618-7.html - принципы защиты операционных систем
2. http://rudocs.exdat.com/docs/index-56877.html - принципы построения операционных систем

3. http://www.winblog.ru/2006/08/21/21080608.html - система парольной защиты
4. http://emanual.ru/download/6661.html - средства безопасности для защиты сервисов
5. http://www.supermegayo.ru/vlomprogr/3.html - Атаки на программное обеспечение.
6. http://www.ab-solutions.ru/artides/information securitv/ - - Методы обеспечения информационной безопасности предприятия.
7. http://www.xnets.ru/plugins/content/content.php?content.113.3 - Сите безопасности Windows
8. http://mitilan.blogspot.ru/2010/03/solaris-10 15.html - Реализация базовых функций по обеспечению безопасности Solaris.
9. http://asher.ru/securitv/book/its/08 - приемы обеспечения безопасности информационных систем.
10. http://itteach.ru/bazi-dannich/sozdanie-zaprosov-v-bd/vse-stranitsi - Запросы. Виды запросов. Создание запросов.
11. http://bd.gvm5cheb.ru/p18aa1.html - Запрос на выборку. Групповые операции.
12. http://www.bnti.ru/showart.asp?aid=660&lvl=03.03. - Технические каналы утечки информации при передаче ее по каналам связи.
1. http://www.bnti.ru/showart.asp?aid=957&lvl=03. - Технические каналы утечки речевой информации.

## 3.3. Общие требования к организации образовательного процесса

Учебная практика проводится сосредоточено преподавателями профессионального и специального циклов (каждый студент имеет индивидуальное рабочее место) на базе филиала.

Сроки проведения практики устанавливаются Филиалом в соответствии с графиком учебного процесса.

В период прохождения учебной практики на обучающихся Филиала распространяются правила охраны труда и правила внутреннего распорядка.

Учебная практика завершается дифференцированным зачетом при условии полноты и своевременности представления отчетов по выполнению практических работ.

Отчеты по выполнению практических работ является документом, на основании которого оценивается уровень знаний и навыков, полученных обучающимся за время прохождения учебной практики.

## 3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по учебной практике: наличие высшего образования, соответствующего профилю профессионального модуля 02 Применение программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах, повышение квалификации не реже 1-го раза в 3 года; прохождение обязательной стажировки в профильных учреждениях не реже 1-го раза в 3 года.

## 3.5. Особенности обучения инвалидов и лиц с ограниченными возможностями здоровья

Учебные занятия инвалидов и лиц с ограниченными возможностями здоровья организуются совместно с другими обучающимися в учебных группах, а также индивидуально, в соответствии с графиком индивидуальных занятий.

При этом необходимо учитывать несколько аспектов:

- особенности нозологии обучающихся инвалидов и лиц с ограниченными возможностями здоровья;
- психоэмоциональное состояния обучающихся;
- психологический климат, который сложился в студенческой группе;
- настрой отдельных обучающихся и группы в целом на процесс обучения.

При организации учебных занятий в учебных группах используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений, создания комфортного психологического климата в группе.

В образовательной деятельности применяются материально-техническое оснащение, специализированные технические средства приема-передачи учебной информации в доступных формах для обучающихся с различными особенностями здоровья, электронные образовательные ресурсы в адаптированных формах.

Специфика обучения инвалидов и обучающихся с ограниченными возможностями здоровья предполагает использование игрового, практико-ориентированного, занимательного материала, который необходим для получения знаний и формирования необходимых компетенций. Подготовка обучающимися заданий для учебных занятий должна сочетать устные и письменные формы в соответствии с их особенностями здоровья.

Для того чтобы предотвращать наступление у обучающихся с инвалидностью и обучающихся, имеющих ограниченные возможности здоровья, быстрого утомления можно использовать следующие методы работы:

- чередование умственной и практической деятельности;

- преподнесение материала с использованием средств наглядности;

- использование технических средств обучения, чередование предъявляемой на слух информации с наглядно-демонстрационным материалом.

При освоении дисциплин инвалидами и лицами с ограниченными возможностями здоровья большое значение должно отводиться проведению с ними индивидуальной работы со стороны преподавателей. В индивидуальную работу включается:

- индивидуальная учебная работа (консультации), то есть дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы;

- индивидуальная воспитательная работа.

Особенности обучения обучающихся с нарушениями опорно-двигательного аппарата.

Для обучающегося, имеющего нарушения опорно-двигательного аппарата, необходимо посоветовать использовать вспомогательные средства для усвоения программы, например, диктофон и другие электронные носители информации.

При проведении аудиторных занятий с обучающимися, имеющими осложнения с моторикой рук, возможно использование следующих вариантов работы:

- обеспечение обучающихся электронными текстами лекций и заданий к учебным занятиям;

- использование технических средств фиксации текста (диктофоны) с последующим составлением тезисов лекции в ходе самостоятельной работы обучающегося, которые они впоследствии могут использовать при подготовке и ответах на учебных занятиях.

Одним из видов работы для обучающихся, испытывающих трудности в письме может быть подготовка к учебным занятиям таких заданий, которые не требуют от них написания длинных текстов ответов. Наиболее оптимальным вариантом такого задания, выполняемого в письменной форме, может служить тестовое задание. Использование тестирования обучающихся необходимо совмещать с обсуждением вариантов ответов.

Контроль знаний можно вести как в устном, так и в письменном виде.

Особенности обучения обучающихся с нарушением слуха.

При организации образовательного процесса со слабослышащей аудиторией рекомендуется использовать следующие педагогические принципы:

- наглядности преподаваемого материала;

- индивидуального подхода к каждому обучающемуся;

- использования информационных технологий;

- использования учебных пособий, адаптированных для восприятия обучающимися с нарушением слуха.

Обучающемуся с нарушением слуха следует предложить занять место на передних партах аудитории, а преподавателю больше времени находиться рядом с рабочим местом этого обучающегося. Учитывая, что такие

обучающиеся лучше понимают по губам, желательно располагаться к ним лицом, говорить громко и четко.

Для повышения уровня восприятия учебной информации обучающимися рассматриваемой группы, рекомендуется применение звукоусиливающей аппаратуры, мультимедийных и других средств. Сложные для понимания темы следует снабжать как можно большим количеством наглядного материала. Особую роль в обучении лиц с нарушенным слухом, играют видеоматериалы. По возможности, предъявляемая видеоинформация может сопровождаться текстовой бегущей строкой или сурдологическим переводом.

Контроль знаний обучающихся указанной нозологии может вестись преимущественно в письменном виде, но для развития устной речи, рекомендуется предложить обучающемуся рассказать ответ на задание в тезисах.

Особенности обучения обучающихся с нарушением зрения.

Специфика обучения слабовидящих обучающихся заключается в следующем:

- необходимо дозировать учебную нагрузку;

- применять специальные формы и методы обучения, технические средства, позволяющие воспринимать информацию, а также оптические и тифлопедагогические устройства, расширяющие познавательные возможности обучающихся;

- увеличивать искусственную освещенность помещений, в которых занимаются обучающиеся с пониженным зрением.

При зрительной работе у слабовидящих обучающихся быстро наступает утомление, что снижает их работоспособность, поэтому необходимо проводить небольшие перерывы или переключение рабочей активности.

При чтении лекций, слабовидящим обучающимся следует разрешить использовать звукозаписывающие устройства и компьютеры, как способ конспектирования, во время занятий. Необходимо комментировать свои жесты и надписи на доске и передавать словами то, что часто выражается мимикой и жестами.

При работе на компьютере следует использовать принцип максимального снижения зрительных нагрузок, дозирование и чередование зрительных нагрузок с другими видами деятельности. Кроме того необходимо использовать специальные программные средства для увеличения изображения на экране или для озвучивания информации.

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей обучающихся:

1. информация по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, на электронном носителе, в печатной форме увеличенным шрифтом и т.п.);

2. доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в форме электронного документа);

3. доступная форма предоставления ответов на задания (письменно на бумаге, набор ответов на компьютере, устно и др.).

При необходимости для обучающихся с инвалидностью и обучающихся с ограниченными возможностями здоровья процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов, а также может быть предоставлено дополнительное время для подготовки ответа на зачете или экзамене.

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

| Результаты обучения | Методы оценки |
|---|---|
| Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.<br>Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.<br>Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.<br>Осуществлять обработку, хранение и передачу информации ограниченного доступа.<br>Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.<br>Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак. | - проверка выполнения практических заданий на занятиях по учебной практике;<br>- проверка документов по учебной практике; |

В случае невыполнения программы учебной практики без уважительной причины либо получения отрицательной характеристики непосредственного руководителя практики от учреждения, обучающийся направляется на учебную практику повторно в свободное от учебы время.

Обучающемуся, не прошедшему учебную практику по уважительным причинам, предоставляется возможность прохождения практики по индивидуальному плану, утвержденному директором / заместителем директора по УМР Филиала.

Студенты, не выполнившие без уважительных причин программу учебной практики, отчисляются из учебного заведения как имеющие академическую задолженность.